

Department of the Army
Headquarters Fort Monroe
Fort Monroe, Virginia 23651-5000

FM Regulation 25-4

2 July 2007

Information Management
FORT MONROE CAMPUS AREA NETWORK (CAN)
CONNECTION POLICY TO THE NON-SECURE INTERNET PROTOCOL ROUTER
NETWORK (NIPRNET)

Summary. This regulation establishes policy for managing the usage of Fort Monroe automation networks and to safeguard the use of government computer equipment from unauthorized use.

Applicability. This regulation applies to all subscribers; military, civilian, and contractors, who have access to Fort Monroe's CAN and all devices connected to it.

Suggested improvements. The proponent of this regulation is the Directorate of Information Management (DOIM). Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, Fort Monroe, ATTN: IMNE-MNR-IM, 59 Patch Road, Fort Monroe, VA 23651-1052. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas For Excellence Program (AIEP) Proposal).

Availability. This regulation is only available at <http://www.monroe.army.mil/Monroe/sites/publications/publications.aspx>.

Content	Paragraph	Page
Purpose.	1-1	1
References	2-1	2
Explanation of abbreviations	3-1	2
Policy	4-1	2
Responsibilities	5-1	2
Procedures	6-1	3
Memorandum of agreement (MOU) or service level agreement (SLA).	7-1	4
Glossary		4

1-1. Purpose.

The purpose of this policy is to protect the Fort Monroe NIPRNET and its users from intentional or inadvertent security compromise.

FM Regulation 25-4

It establishes the rules for devices, sub-networks, and enclaves to obtain and maintain connectivity to the Fort Monroe network and includes rules for hardware, software, and user performance. This policy requires connected devices or subnets to be accredited, maintained and operated in accordance with (IAW) the accreditation terms, and become part of the Fort Monroe CAN. As such, they are subject to the Army-level and Fort Monroe Information Assurance Security staff monitoring and enforcement. Adherence to this policy will reduce the risk of alteration, theft, or destruction of data and denial of service.

2-1. References.

- a. AR 25-1, Army Knowledge Management and Information Technology, 15 Jul 2005.
- b. AR 25-2, Information Assurance, 14 Nov 2003.
- c. Interim Department of Defense (DoD) Information and Assurance (IA) Certification and Accreditation (C&A) Process Guidance, 6 Jul 2006.

3-1. Explanation of abbreviations. The glossary contains abbreviations used in this regulation.

4-1. Policy. Network connection rules must be consistent with network accreditation criteria.

- a. Accreditation is the culmination of a strict procedure that organizes and configures automated information systems (AIS) to achieve an acceptable level of risk. Networks must be accredited before they can be made operational.

- b. All connected devices, local area networks (LANs) and enclaves, regardless of the command affiliation of their owner, must adhere to a single connection rule policy.

5-1. Responsibilities.

- a. The Fort Monroe DOIM will verify compliance with this policy and impose restrictions on connected systems for noncompliance.

- b. The Fort Monroe Designated Approval Authority (DAA) will—

- (1) Ensure the Fort Monroe CAN is compliant with the system certification stipulations.

(2) Decide if IA measures taken have mitigated security risks to the Fort Monroe CAN is sufficient to warrant operation on the network.

(3) Grant accreditation and any changes to the network that affect security before implementation.

c. The Installation Assurance Manager(IAM) will—

(1) Enforce adherence to the accreditation terms and require tenants to provide special equipment necessary to support the tenant requirements for network connection.

(2) Authorize and verify security features by automated vulnerability scanning, modem identification scanning, and physical inspection to check for compliance with the Fort Monroe connectivity policy.

(3) Authorize disconnection or limit the connection of devices, LANs, and enclaves that fail to meet terms of the accreditation or the MOA.

d. The staff sections Systems Administrator(SA) or organizations Information Management Officer(IMO) will keep an inventory of laptops, ensure hard drives are encrypted, and install current antivirus definitions and patches on the devices weekly.

6-1. Procedures.

a. Any activity requesting connection of a device, LAN, or enclave to the Fort Monroe CAN will, prior to connection, provide a description (pictorial and narrative) of the system to the installations DAA. This description will show the internet protocol(IP) address assigned to each bridge, router, and/or switch connected to the network, and all external connections and their locations. Additionally, the description should strive to associate IP sub-networks to physical segments for the switches, etc.

b. After connection is authorized, any required updates or changes to the network will be submitted to the installation IAM for approval and incorporation into the installation site Certification and Accreditation plan before implementation. If the IAM determines that the new or changed system is not compliant with Fort Monroe policy, they may require the requesting agency to make the system compliant.

c. The DAA will determine if connecting the new or changed system will result in the need to reaccredit either or both systems.

d. Certification documentation is required for any laptop brought to Fort Monroe that requires network access. The organizations IMO will provide documentation to DOIM IA Office.

e. Tenant activities and proponents for fielded systems (Department of the Army (DA) or DoD) will comply with the installation policy and may be required to provide additional information.

7-1. Memorandum of agreement (MOA) or service level agreement (SLA).

a. The requesting unit's DOIM or IA personnel, and the Fort Monroe DOIM will develop an MOA or SLA that establishes the operating conditions that must be maintained by both parties. This document will describe all of the conditions necessary to maintain an optimum, secure, non-interfering connection that conforms to the Fort Monroe accreditation.

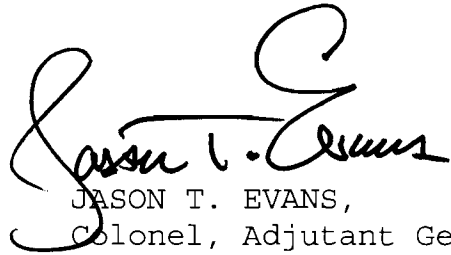
b. Any changes in the requesting unit's system that affects network integrity or security will require approval by the DAA before implementation.

c. Connection to the installations network constitutes consent to verification of security features including automated vulnerability scanning, modem identification scanning, physical inspection and network activity monitoring. Failure to comply with Fort Monroe policies, Army regulations, and/or DoD memorandums, may result in disconnection from the network infrastructure. Exceptions to policy must be requested, in writing, to the Director, Information Management.

GLOSSARY

AIS	automated information system
AR	army regulation
CAN	campus area network
DA	Department of the Army
DAA	designated approval authority
DoD	Department of Defense
DOIM	Directorate of Information Management
IA	information assurance

IAM	Information Assurance Manager
IAW	in accordance with
IMO	Information Management Officer
IP	internet protocol
LAN	local area network
MOA	memorandum of agreement
NIPRNET	non-secure internet protocol router network
SA	systems administrator
SLA	service level agreement



JASON T. EVANS,
Colonel, Adjutant General
Commanding

DISTRIBUTION:

<http://www.monroe.army.mil/Monroe/sites/publications/publications.aspx>